UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/494,507	01/31/2000	Yoshimi Baba	CS-02-000131	3553

22712 7590 01/15/2004

PAUL A. GUSS
PAUL A. GUSS ATTORNEY AT LAW
775 S 23RD ST FIRST FLOOR SUITE 2
ARLINGTON, VA 22202

EXAMINER	
ADAMS, JONATHAN R	
ART UNIT	PAPER NUMBER
2134	7

DATE MAILED: 01/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/494,507	**Applicant(s)** BABA, YOSHIMI
	Examiner Jonathan R Adams	**Art Unit** 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/31/2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) □ The translation of the foreign language provisional application has been received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

11/12/04
Primary Examiner

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) □ Interview Summary (PTO-413) Paper No(s). _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 1-4,13 rejected under 35 U.S.C. 102(b) as being anticipated by "Intrusion Detection" by Terry Escamilla (hereafter referred to as "Intrusion").

As to claims 1, and 4, Intrusion teaches a system for monitoring a network based on IP comprising:

Attack detection means / Intrusion Detection

Acquiring/Storing IP Packets / Network traffic is usually obtained by... (Page 174, "Data Source", Line 2 et seq., Intrusion)

Monitoring the stored IP packets / Network packet-based IDSs filter ... (Page 308, "Discovery and Detection", Line 4 et seq., Intrusion)

Processing means... / Processing means is a requisite inherent to all computer based systems

Effecting a predetermined process / Custom responses can be designated for each event of interest (Page 308, "Discovery and Detection", Line 15 et seq., Intrusion)

Holding an algorithm for detecting / Intrusion Detection code (Page 194, Line 10 et seq., Intrusion)

Generating a report output / IDS prints reports ... (Page 308, "Discovery and Detection", Line 21 et seq., Intrusion)

As to dependent claims 2 and 3:

Although Intrusion teaches receiving IP packets, it does not explicitly teach receiving all IP packets. However, this feature is inherent to all intrusion detection systems and is necessary to perform the functions they carry out.

Receiving only IP packets / As broadly as stated, the invention as disclosed in Intrusion implemented in a network based solely on Internet Protocol would receive only IP packets.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6-12, 14-29

✓ Claims 5 rejected under 35 U.S.C. 103(a) as being unpatentable over Intrusion in view of Cheswick.

Intrusion teaches the use of coupling an intrusion detection system with a firewall (Page 194, Line 5 et seq., Intrusion) in a system for monitoring and detecting crackers in a network based on IP. Intrusion also teaches the classification of network data in pattern matching detection including general regular expressions (Page 170, Line 17 et seq., Intrusion). Intrusion does not explicitly teach classifying the acquired IP packets by source/destination IP. Cheswick teaches the classification of IP packets by source/destination IP as a general regular expression packet-filtering rule (Section 3.3, Line 5 et seq., Cheswick). It would have been obvious to a person of ordinary skill in the art at the time of invention to include the classification by source/destination as a general regular expression for use in the coupled IDS/Firewall system. One of ordinary skill in the art would have been motivated to include the classification by source/destination because such a classification is notoriously well known in the art as a packet-filtering rule to prevent many known forms of attacks.

As to claims 6-12:

The examiner takes official notice of both the motive and modification necessary to use the various patterns and characteristics listed in claims 6-12 as a means for detecting their associated attacks within the IDS/Firewall combination disclosed in Intrusion.

Intrusion teaches the use of coupling an intrusion detection system with a firewall (Page 194, Line 5 et seq., Intrusion) in a system for monitoring and detecting general types of cracker attacks based on their known patterns and characteristics in a network based on IP. Intrusion also discloses a means for detecting attacks known as "syn-flood" (Page 267, Line 6 et seq., Intrusion), "Fragmented IP Packets" (Page 268, Intrusion), and "Brute force" (Page 172, Line 23 et seq., Intrusion). Intrusion does not explicitly teach the patterns and characteristics by which the abovementioned attacks are detecting, nor does it teach the other attack methods listed in the claims or their associated patterns and characteristics. It would have been obvious to a person of ordinary skill in the art at the time of invention to use the various patterns and characteristics listed in the claims as a means to detect their well known associated attacks. One of ordinary skill in the art would have been motivated to use these various patterns and characteristics as a means for detecting their associated attacks because attacks are defined by the characteristics they entail, and therefor must be detected in this manor.

As to claims 14 – 17, 19, 20, 22, 23, 25, 26, 27:

The examiner takes official notice of both the motive and modification necessary to reject packets based on the IP packet characteristics detected by the IDS.

Intrusion teaches the use of coupling an intrusion detection system with a firewall (Page 194, Line 5 et seq., Intrusion) in a system for monitoring and detecting general types of cracker attacks based on their known patterns and characteristics in a network based on IP. Intrusion does not explicitly teach the means for rejecting IP packets based on the IP header characteristics associated with the well-known specific attacks listed in claims. It would have been obvious to a person of ordinary skill in the art at the time of invention to reject packets based on the IP packet characteristics detected by the IDS. One of ordinary skill in the art would have been motivated to reject packets in this manor because rejecting packets based on IP characteristics is well known in the art as a method by which packet filtering firewalls provide protection.

As to claims 18, 21, 24:

The examiner takes official notice of both the motive and modification necessary to filter packets from the source of the attack for a longer period of time than packets to the attack destination.

Intrusion teaches the use of coupling an intrusion detection system with a firewall (Page 194, Line 5 et seq., Intrusion) in a system for filtering IP packets associated with an attack. Intrusion does not explicitly teach to filter packets from the source of the attack for a longer period of time than packets to the attack destination. It would have been obvious to a person of ordinary skill in the art at the time of invention to filter packets from the source of the attack for a longer period of time than packets to the attack destination. One of ordinary skill in the art would have been motivated to filter packets from the source of the attack for a longer period of time than packets to the attack destination because it is obviously beneficial for the attack destination being protected by the network monitoring system to return to packet receiving status immediately after the period of time characteristic to a certain type of attack. Similarly, it is obviously beneficial to reject packets as long as possible from the source of an attack, or until other action can be taken.

As to claim 28, it recites concomitance elements of previously rejected claims and therefor fail to distinguish over them accordingly. See above for the specifics of the rejection.

As to claim 29, it further recites:

Further comprising a packet filter / filtering capabilities to received packets (Page 194, Line 5 et seq., Intrusion)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (703) 305-8894. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306 Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.